BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	
	)	

COMMENTS OF THE SATELLITE INDUSTRY ASSOCIATION

Satellite Industry Association
225 Reinekers Lane
Suite 600
Alexandria, VA 22314
(703) 739-8358

November 8, 2004

TABLE OF CONTENTS

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	
	)	

COMMENTS OF
THE SATELLITE INDUSTRY ASSOCIATION

I. INTRODUCTION AND SUMMARY

The Satellite Industry Association ("SIA") hereby comments on the Federal Communication Commission's ("Commission" or "FCC") *Notice of Proposed Rulemaking* in the above-mentioned docket ("*CALEA Broadband NPRM*").[1] SIA is a U.S.-based trade association representing the leading satellite manufacturers, system operators, service providers, and launch service companies. SIA serves as an advocate for the commercial satellite industry on regulatory and policy issues common to its members. With its member companies providing a broad range of manufactured products and services, SIA represents the unified voice of the U.S. commercial satellite industry.[2]

SIA and its members support the Commission's objective in this proceeding to implement CALEA fully and to ensure law enforcement's continued ability to surveil packet-

[1] *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking, FCC 04-187 (Aug. 9, 2004) ("*CALEA Broadband NPRM*").

[2] SIA Executive Members include: The Boeing Company; Globalstar, L.P.; Hughes Network Systems, Inc.; ICO Global Communications; Intelsat Ltd.; Iridium Satellite LLC, Lockheed Martin Corp.; Loral Space & Communications Ltd.; Mobile Satellite Ventures; Northrop Grumman Corporation; PanAmSat Corporation; Verestar Inc. and SES-Americom, Inc. SIA's Associate Members include Eutelsat Inc., Inmarsat Ltd., and New Skies Satellites Inc.

mode communications that are within the ambit of CALEA.[3] The satellite industry has cooperated closely with law enforcement to provide appropriate interception capabilities when requested. In addition, if CALEA obligations are determined to apply as a result of this proceeding to broadband Internet access and managed voice over Internet Protocol ("VoIP"), our members are committed to providing the assistance capabilities in a timely and appropriate manner.

The *CALEA Broadband NPRM* is designed to "remove…uncertainty that is impeding CALEA compliance" and to "examine the appropriate legal and policy framework of CALEA, particularly with respect to new packet mode technologies and services."[4] The *NPRM* recognizes that the FCC's statutory authority to expand CALEA obligations is tied to services that replace "a substantial portion of the local telephone exchange service."[5] Employing that test, the Commission tentatively concludes that "facilities-based providers of any type of broadband Internet access service, whether provided on a wholesale or retail basis, are subject to CALEA."[6]

The *NPRM* only briefly mentions satellite services, acknowledging relevant statutory exemptions,[7] but proposes to perpetuate the current individually negotiated "system-by-system" arrangements.[8] But, there are important and different players in the satellite industry – spacecraft

[3] *See CALEA Broadband NPRM*, ¶ 1.

[4] *Id.*, ¶ 30.

[5] *Id.*, ¶ 1; *see also* 47 U.S.C. § 1001(8)(B)(ii).

[6] *CALEA Broadband NPRM*, ¶ 37 (internal citations omitted).

[7] *Id.*, ¶ 37 & n.80 (providers that "sell or lease mere transmission facilities on a non-common carrier basis," such as "bare space segment capacity," have no obligation to provide the CALEA assistance capabilities.).

[8] *Id.*, ¶ 86.

owner-operators, and the intermediate providers of various types of services via space segment leased or otherwise acquired from the spacecraft owner-operators. The FCC must ensure that any final rules appropriately recognize service and technical distinctions that directly bear on CALEA's applicability and scope. Moreover, to reduce the administrative burden on both law enforcement and Fixed Satellite Service ("FSS") licensees, any such rules should be appropriately simple and equally applicable to similarly-situated licensees.

Our comments herein apply primarily to the FSS sector of the industry.[9] As an initial matter, SIA agrees that many offerings by FSS licensees are outside of CALEA.[10] SIA concurs with the Commission's recognition that it may extend CALEA only to offerings "substantial[ly]" replacing local exchange services,[11] which excludes non-public and long-haul capacity offered by FSS owner-operators. Most FSS offerings do not substantially replace local exchange services in the last mile, and thus, are not subject to CALEA.

To the extent that public broadband Internet access services and managed VoIP services provided via satellite to end users are covered by CALEA, SIA urges the Commission to cooperate with *all* industry associations or standards-setting bodies to develop platform-independent CALEA safe harbor standards that are based on encoding and transmission protocols used by both satellite-based and terrestrial providers. In addition, the Commission should clarify the precise broadband content obligations of CALEA-covered providers when complying with a lawful intercept demands; that the term "call identifying information," as

[9] Mobile-Satellite Service ("MSS") licensees are subject to CALEA under existing rules, and have concluded system-specific arrangements with law enforcement.

[10] Bare transponder service, for example, is not subject to CALEA. Obviously, it is impractical to retrofit spacecraft for CALEA compliance once it is in orbit, especially considering that law enforcement always has the option to intercept communications on the ground.

[11] *CALEA Broadband NPRM*,¶ 37 & n.80.

applied to the broadband Internet access provider, includes only information from the transport layer headers; and that the managed VoIP application provider bears the responsibility for providing any call-identifying information.

Finally, the Commission should establish a reasonable time period for satellite-based providers of broadband Internet access and managed VoIP services to achieve CALEA compliance. Specifically, the Commission should require compliance by a date one year after (1) one or more industry associations or standard-setting organizations establish safe harbor safeguards that are generally agreed to meet the CALEA capability requirements of Section 103, or the date on which the Commission's order resolving any petitions filed pursuant to Section 107(b) takes effect; (2) the Attorney General issues a final notice of capacity applicable to entities providing any services the Commission finds are subject to CALEA in this proceeding; and (3) the Commission establishes system security and integrity rules applicable to such entities pursuant to CALEA Section 105.

II. MOST FSS SERVICES, EQUIPMENT AND FACILITIES ARE NOT SUBJECT TO CALEA.

A. The NPRM Properly Acknowledges that CALEA Exempts Bare Space Segment, Non-Public and Internetworking FSS Capacity.

The *NPRM* does not, and could not, alter existing CALEA exemptions as applied to the offering of FSS capacity. Thus, SIA supports the FCC's acknowledgement that entities which "sell or lease mere transmission facilities on a non-common carrier basis"—including, specifically "bare space segment capacity"—have no obligation to provide CALEA assistance

capabilities.[12] The Commission has long classified bare space segment capacity as a facility, not a service,[13] and thus it is not subject to CALEA requirements.

Similarly, CALEA assistance obligations do not extend to "equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers."[14] Thus, FSS capacity that is either offered in support of private networks or that is leased to "communications intermediaries," such as interexchange carriers, Internet access providers, Internet backbone providers, and facilities resellers, is exempt from CALEA. This includes capacity that FSS owner-operators provide when not in contractual privity with public end-user subscribers.[15]

B. The NPRM Properly Does Not Expand CALEA Obligations Beyond Offerings That Substantially Replace Local Exchange Services in the "Last Mile."

Congress authorized the FCC to extend CALEA obligations to an entity providing wire or electronic communication switching or transmission services if the agency finds that such a service is a "replacement for a substantial portion of the local telephone exchange service."[16] The *CALEA Broadband NPRM* proposes to expand CALEA upgrade obligations to broadband Internet access service providers, because that functionality replaces narrowband dial-up Internet

---

[12] *Id.*

[13] *Domestic Fixed-Satellite Transponder Sales,* Memorandum, Opinion Order and Authorization, 90 F.C.C.2d 1238 (1982), *aff'd Wold Communications, Inc. v. FCC*, 735 F.2d 1465 (D.C. Cir 1984).

[14] 47 U.S.C. § 1002(b)(2)(B).

[15] In such circumstances, intermediaries, which ultimately publicly offer capacity directly to subscribers, may already be subject to affirmative CALEA obligations.

[16] 47 U.S.C. § 1001(8)(B)(ii). The FCC describes its authority as limited to services that substitute for "any portion of an individual subscriber's functionality previously provided via 'plain old telephone service'" ("POTS"). *CALEA Broadband NPRM*, ¶ 1.

access, previously provided by the local exchange.[17] The FCC defines "broadband" service as "service…having the capability to support both upstream or downstream speeds in excess of 200 kbps *in the last mile*."[18]

SIA notes that, due to its inherent economies and technological advantages, FSS capacity often is deployed for long-haul traffic. FSS's large beam size, and efficiencies for multipoint, are more closely analogous to interexchange providers and services, which are often exempt from CALEA. This is especially true for services provided to intermediaries, as opposed to public end users. So, under the proposed rules, when FSS owner operators supply long-haul transport to broadband Internet access providers, such transport is neither a replacement for the local exchange,[19] nor the final mile, and thus not a "broadband" service subject to CALEA.[20]

---

[17] *CALEA Broadband NPRM,* ¶¶ 44, 48.

[18] *CALEA Broadband NPRM,* ¶ 35 & n.77 (emphasis added).

[19] FSS provided to intermediaries, and not to subscribers, is not a replacement for "local exchange" service. *See* H.R. Rep. No. 103-827(I), at 21 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3498 ("The *only* entities required to comply with the [CALEA] functional requirements are telecommunications common carriers, the components of the *public switched network* where law enforcement agencies have always served most of their surveillance orders") (emphasis added); *id.* at H.R. Rep. No. 103-827(I), 26, reprinted in 1994 U.S.C.C.A.N. 3489, 3503 (CALEA covers carriers that "allow[ ] the customer to obtain access to a *publicly switched network* ... On the other hand, for communications handled by multiple carriers, a carrier that does not originate or terminate the message, but merely interconnects two other carriers, is *not* subject to the requirements for the interconnection part of its facilities") (emphasis added*).*

[20] Law enforcement has multiple options when seeking to tap communications relayed by a transponder. Agents generally find wiretapping more convenient at the facilities of service providers upstream or downstream from a satellite owner-operator. *See, e.g.*, Letter from Joan M. Griffin, Counsel to COMSAT General Corporation, Lockheed Martin Global Telecommunications LLC and COMSAT New Services ("COMGEN"), and John B. Reynolds III, Counsel to Intelsat LLC, Intelsat MTC LLC and Intelsat Government Solutions Corporation ("Intelsat") to the U.S. Departments of Justice and Homeland Security and the Federal Bureau of Investigation, IB Docket No. 04-235 (filed Oct. 5, 2004) (attached as Exh. 1 to Letter from Myla R. Saldivor-Trotter, DOJ to Marlene H. Dortch, Secretary, FCC (filed Oct. 7, 2004)) (explaining that law enforcement would not find it useful to work through Intelsat to execute interceptions in a proceeding concerning Intelsat's acquisition of COMGEN in which Executive Branch agencies did not require a National Security Agreement). In addition, depending on the circumstances, satellite communications may also be accessed directly by setting up a "sniffer" earth station anywhere within the satellite footprint.

Put differently, not all satellite public packet-switched offerings by FSS licensees fall within the proposed expansion of CALEA.

III. IF THE COMMISSION CONCLUDES THAT PACKET-BASED, SATELLITE-DELIVERED, MANAGED VOIP AND BROADBAND INTERNET ACCESS SERVICES ARE COVERED BY CALEA, PLATFORM-INDEPENDENT SAFE HARBOR COMPLIANCE STANDARDS SHOULD BE DEVELOPED.

The Commission's *NPRM* focuses on the application of CALEA to broadband Internet access and managed VoIP services.[21] As noted above, these services represent only a small portion of the broad spectrum of satellite facilities and services that SIA members provide today.

A. The Commission Should Not Mandate System-by-System Agreements in the Context of Broadband Internet Access and Managed VOIP Services Provided over FSS Platforms.

Contrary to the Commission's tentative conclusion in the *CALEA Broadband NPRM*, SIA believes that there is no need, as a general matter, for the Commission to mandate that providers of broadband Internet access and managed VOIP services provided over FSS platforms directly to end users ("Satellite Broadband Providers") negotiate system-by-system CALEA compliance agreements with law enforcement agencies.[22] While the Commission correctly observes that such agreements have been reached between law enforcement authorities and some Mobile Satellite-Service ("MSS") service providers, SIA believes that it would be unnecessarily burdensome for the Commission to mandate such a result in the context of broadband Internet access and managed VOIP services provided directly to end users over FSS platforms. There is also no need to craft individualized agreements to take into account unique Satellite Broadband Providers' networks because both terrestrial and satellite-based packet-mode networks use the same encoding and transmission protocols. Rather, the Commission should focus its effort on

---

[21] *CALEA Broadband NPRM*, ¶ 37.

[22] *CALEA Broadband NPRM*, ¶ 86.

developing in cooperation with industry groups safe harbor CALEA compliance standards that apply at the router, without regard for whether the router is part of a satellite-based or terrestrial network.

In this respect, satellite technology is effectively a "red herring" that should not distract either the Commission or standard-setting bodies from the goal of creating platform-independent safe harbor compliance standards for broadband Internet access and managed VoIP services. To route broadband Internet access and managed VoIP traffic to and from their earth stations, Satellite Broadband Providers use standard routers that are identical to those used by terrestrial packet-mode network operators, such as those operated by DSL-based or cable modem-based direct providers of broadband Internet access. Because broadband Internet access and managed VoIP services provided over an FSS platform aggregate traffic at terrestrial hubs tied to standard routers, there is no need for an individualized CALEA compliance standard for satellite technology. Properly-designed CALEA compliance standards that can be incorporated into standard routers should be equally suitable for use by satellite-based as for terrestrial broadband Internet access and managed VoIP providers.

That said, SIA acknowledges that, in limited circumstances, system-specific agreements may be appropriate. Clearly, they have already allowed several MSS service providers to implement CALEA capabilities in their networks. For Satellite Broadband Providers, as defined above, while no such individualized agreements should generally be needed, they may have a useful role in implementing CALEA depending on the unique characteristics of a specific system that might not support a router-based solution. For example, such an agreement might be necessary if (1) a satellite-based service provider were to launch a broadband Internet access or managed VoIP service that used a network architecture in which packets do not pass through a central hub on the ground; or (2) a satellite-based service provider were to launch a new

broadband Internet access or managed VoIP service based on a non-standard transmission protocol that was not compatible with the existing packet-based CALEA standards or CALEA-compliant routers.

B. The Commission Should Clarify Limited Aspects of the CALEA Framework as it Applies to Managed VoIP and Broadband Internet Access for the Benefit of Providers and Standard Setting Organizations.

1. The Commission Should Clarify the Scope of the CALEA Capability Requirements as They Apply to Broadband Internet Access and Managed VoIP Services Provided Directly to End Users.

The Commission seeks comment on whether existing CALEA compliance standards available for packet-mode communications should be used as safe harbors under Section 107(a) for broadband Internet access and managed VoIP services.[23] CALEA Section 103(a) requires carriers to incorporate into their networks the capability to (1) isolate and enable the government to intercept call content information, as described in Section 103(a)(1); and (2) isolate and enable the government to intercept "call-identifying information" that is reasonably available to the carrier, as described in Section 103(a)(2). The Commission's questions are best addressed separately for each of these elements.

a. Content Information

In cases where law enforcement has obtained lawful authorization to receive the full content of a subject's communications, the issues surrounding CALEA compliance are easiest to resolve. The Commission and the United States Court of Appeals for the District of Columbia Circuit ("D.C. Circuit") have long recognized that substantial privacy issues would arise if a carrier were to deliver call content information to a law enforcement agency, based on an authorization for that agency to receive only call-identifying information, *e.g.*, under a pen

[23] *CALEA Broadband NPRM*, ¶ 81.

register.[24] In cases where law enforcement has received authorization to obtain the entire content, however, compliance with CALEA's Section 103(a)(1) becomes more straightforward. In such a case, a variety of network analyzer utilities exist today that can capture packets with particular source or destination IP addresses, and output them in a standardized format, such as LIBCAP. Once captured, the complete packet stream can be delivered to law enforcement for analysis without difficulty. Of course, this assumes that delivery occurs contemporaneously with the communication. Long term storage of the packet stream would be very costly, if not entirely impractical.

b. Call-Identifying Information

(i) Managed VoIP

In the managed VoIP context, the Commission should clarify that it is the managed VoIP application provider, which controls the gateway between the IP and circuit switched TDM networks, that bears the obligation to provide such call-identifying information to law enforcement.[25] CALEA requires carriers to provide call-identifying information only to the extent that it is "reasonably available" to the carrier.[26] In the case of VOIP provided over a satellite-based broadband Internet access service, only the VoIP application provider will have access to the call-identifying information embedded in the packets, which it can access at the

---

[24] *E.g.*, *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 465 (D.C. Cir. 2000) ("CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is 'not authorized to be intercepted.'") (quoting 47 U.S.C. § 1002(a)(1)-(3)); *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Third Report and Order, FCC 99-230, 14 FCC Rcd 16794 (1999), at ¶ 55 (recognizing the privacy concerns such actions would create).

[25] SIA believes that the Commission intended this result when it tentatively concluded that "providers of managed VoIP services" are subject to CALEA. *CALEA Broadband NPRM*, ¶ 56.

[26] CALEA Section 103(a)(2), 47 U.S.C. § 1002(a)(2).

gateway between the IP and circuit-switched TDM networks. The broadband Internet access provider, in contrast, merely provides transport between the customer's premises and the IP address specified for the gateway; call-identifying information in this context is not "reasonably available" to the broadband Internet access provider because it is embedded within the content of the packets themselves. It would be impossible (or at the very least, highly impractical), for the transport provider to decode each packet, and separate the Session Initiation Protocol (SIP) or H.323-encoded call-identifying information from the bearer information also contained in the packet. Because of the resource intensity of such activities, at a minimum, a broadband Internet access provider would need to make significant modifications to its network to incorporate this ability.[27]

The Commission also seeks comment on whether it should clarify the meaning of the term "call identifying information" for broadband Internet access and managed VoIP services.[28] SIA believes that, with respect to managed VOIP services, the term "call-identifying information" is adequately clear and has been applied successfully in the development of the existing packet-mode compliance standards the Commission identifies.[29] As the Commission notes, "[f]or VoIP, the concept of 'call' seems well understood, and we might expect call-identifying information to include who called whom when for how long, and concepts similar to

---

[27] *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Order on Remand, FCC 02-108, 17 FCC Rcd 6896, ¶ 80 (holding that information is not "reasonably available" if access would require "significantly modifying the carrier's network."

[28] *CALEA Broadband NPRM*, ¶ 67.

[29] The Commission in particular identifies TIA's J-STD-25, J-STD-025A, and J-STD-025B, ATIS standards T1.724 and T1.678, and CableLabs PacketCable specifications PKT-SP-ESP-I01-991229, PKT-SP-ESP-I01-030815 and PKT-SP-ESP-I03-040113. *See CALEA Broadband NPRM*, ¶ 81, n.193 & Appendix D.

call-identifying information for circuit-mode calls."[30] The CALEA compliance standards developed to date have focused on CALEA implementation for packet voice communication, and create methods by which call-identifying information elements analogous to those identified for circuit-switched networks may be gathered and relayed to law enforcement agencies from SIP, H.323, or analogous signaling information embedded within managed VoIP packets. These CALEA standards represent an important step toward implementing CALEA capabilities for packet voice communications, including managed VoIP.[31]

(ii) Broadband Internet Access

Further work will need to be done to clarify the term "call-identifying information," however, if the Commission ultimately adopts its tentative conclusion to subject broadband Internet access to CALEA obligations generally. Without additional clarification of this statutory term, these standards cannot yet readily be applied in the context of ordinary web browsing, file downloads, and email communications for which customers commonly use broadband Internet access connections today. Furthermore, because such packets are not part of a "call," not all of the information available from such packets readily maps to equivalent elements of call-identifying information defined for either circuit-switched or VoIP calls.[32]

Specifically, the Commission should clarify that, for such packets, the term "call-identifying information" includes the information contained in the transport layer headers, which

---

30 *CALEA Broadband NPRM*, ¶ 66.

31 For the reasons discussed above in this section, to the extent the Commission determines that post-connection dialed digit extraction ("DDE") constitutes call-identifying information that must be provided, *see CALEA Broadband* NPRM, ¶¶ 82-83, the Commission should clarify that it is the VoIP application provider that bears the responsibility for gathering this information under CALEA.

32 Indeed, J-STD-025B, for example, explicitly states, with respect to packet data call content channel delivery, that "[t]he text in this section may not apply to an IP network." J-STD-025B, at 135 (§ B.6).

includes source and destination IP addresses, the TCP/UDP port information, IP subprotocol information, and the header's time stamp. This is the only identifying information reasonably available to the broadband access provider. Often the remaining content of the packet is encrypted, or encoded using proprietary technologies.[33] Thus, any additional information that might be available from the content of the packet is frequently unavailable to the Satellite Broadband Provider and would, in any event, require the Satellite Broadband Provider to read the content of each packet (if possible), extract the necessary information from the remaining content of the packet, and deliver only the authorized information to law enforcement.

Call-identifying information from the packet transport layer headers, in contrast, can be summarized for delivery to law enforcement using Cisco's Netflow utility[34] or an equivalent third party solution such as sFlow,[35] either of which can provide, for each of the subject's Internet sessions, the source and destination IP address, the time of the session and how long it lasted, the port used, and the number of packets sent and received.

2. All Standards-Setting Bodies Should Be Recognized

CALEA establishes a clear statutory framework governing the development of standards and technical requirements to comply with the surveillance capabilities the statute mandates.

---

[33] Microsoft, for example, uses proprietary encoding technologies for the content of packets sent or received by Internet Explorer and Windows Media Player, or for file downloads.

[34] *See* http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml (visited Nov. 4, 2004) ("NetFlow provides valuable information about who is using the network, what applications are used, when the network is utilized and where traffic is going on the network").

[35] *See* http://www.sflow.org/sFlowOverview.pdf (visited Nov. 4, 2004) ("sFlow provides a network-wide view of usage and active routes. It is a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location."). sFlow takes advantage of the statistical properties of packet sampling and can be modeled using statistical sampling theory. This means that the sFlow traffic monitoring system produces statistically quantifiable measurements. *See* http://www.sflow.org/about/sampling_theory.php (visited Nov. 8, 2004).

Specifically, Section 107(a) of CALEA establishes a compliance "safe harbor" for carriers, equipment manufacturers, and support service providers that are "in compliance with publicly-available technical requirements or standards adopted by an industry association or standards-setting organization, or by the Commission . . . ."[36] Section 107(b) establishes a clear statutory preference for private-sector development of such standards, authorizing the Commission to develop such "safe harbor" standards only "if industry associations or standard-setting organizations fail to issue technical requirements or if a Government agency or any other person believes that such requirements or standards are deficient" and petitions the Commission to intervene.[37]

Today, reflecting the global nature of the industry, there are a tremendous number of bodies – both U.S.-based and non-U.S.-based – developing packet encoding and transmission protocols, packet capture and network analysis tools, and output file format standards. For example, the Internet Engineering Task Force ("IETF"), a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet"[38] is open to any interested individual and has been particularly active in establishing standards that are useful themselves in complying with CALEA, in addition to forming integral parts of other CALEA compliance standards, such as J-STD-025, J-STD-025A, and J-STD-025B.

---

[36] 47 U.S.C. § 1006(a).

[37] 47 U.S.C. § 1006(b).

[38] "Overview of the IETF," *available at* http://www.ietf.org/overview.html (visited Nov. 4, 2004).

Despite past success, the *CALEA Broadband NPRM* expresses reservations about standards bodies and suggests threshold qualifications for acceptable industry bodies.[39] SIA believes this would be unlawful, unworkable and unnecessary. The statute places no limitations on the definitions of "industry association" or "standard-setting organization," and the FCC simply may not exceed the authority delegated by Congress.

Furthermore, reliance on broadly-defined industry associations and standard-setting organizations wisely reflects Congressional recognition that the rapid growth and evolution of packet-mode technology and services make private sector input particularly useful and appropriate. Given the need for carriers to maintain compliance with the CALEA capabilities as their networks evolve, it would make little sense to reject creative potential solutions simply because they were developed by this or any other standard-setting organization the Commission has not "sanctioned" for that purpose.

Finally, such limitations are unnecessary. Section 107(b) of CALEA already authorizes the agency to revise or reject those standards that fail to achieve the full complement of surveillance capabilities prescribed under CALEA Section 103(a). Moreover, SIA members remain willing to cooperate with law enforcement bodies in good faith.[40] To the extent a dispute

---

[39] *CALEA Broadband NPRM*, ¶ 80.

[40] The Commission cites the Law Enforcement Petitioners objections to the processes of standard-setting organization bodies that "did not agree with Law Enforcement's position that industry is required to provide the same level of capability for packet-mode technology as it does for circuit-switched technology." *CALEA Broadband NPRM*, ¶ 78 (quoting Petition at 35). Failure of a standard-setting organization to accept uncritically one interested party's views on this or any other point to the exclusion of others does not constitute a reason to disqualify that organization. Indeed, adoption of any such unilateral and outcome-determinative veto would undermine Congresses preference, embodied in Section 107, for cooperative public-private sector safe-harbors.

arises, the Commission should clarify any ambiguous statutory terms[41] and allow standard-setting organizations to incorporate that refinement into its standard.

IV. THE COMMISSION SHOULD ESTABLISH A REASONABLE TIME PERIOD FOR SATELLITE BROADBAND PROVIDERS TO ACHIEVE CALEA COMPLIANCE.

As the Commission correctly observes, adoption of the *CALEA Broadband NPRM's* tentative conclusions regarding managed VoIP and broadband Internet access providers would expand CALEA to cover numerous entities—such as Satellite Broadband Providers—never previously subject to CALEA. In particular, newly covered entities would be obliged to meet the capability requirements of Section 103, the capacity requirements of Section 104, and the system security requirements of Section 105.[42] These mandates cannot be achieved instantaneously. Rather, substantial effort by the Commission, standards bodies, law enforcement agencies, equipment manufacturers, and the newly-identified entities themselves will be required to achieve each of these steps.

With respect to Section 103, once the FCC has clarified key ambiguities in its statutory interpretation and proposed rules, industry associations and standard setting organizations must be given adequate time to incorporate these findings into their CALEA compliance standards, to the satisfaction of the law enforcement community, carriers, and the Commission alike. Finally, equipment manufacturers must have time to incorporate these compliance standards into their products.

Meanwhile, Section 104 prescribes a detailed process under which the Attorney General is charged, within one year of CALEA's enactment, with the responsibility for publishing in the

---

[41] SIA agrees that statutory terms such as "call-identifying information" and "reasonably achievable" could, in some circumstances, be ambiguous. *CALEA Broadband NPRM*, ¶ 78.

[42] *CALEA Broadband NPRM*, ¶ 140.

Federal Register and providing to appropriate telecommunications industry associations and standard-setting organizations notice of the actual number of communication interceptions, pen registers, and trap and trace devices that the Attorney General estimated would be conducted within four years of CALEA's enactment, as well as the estimated maximum capacity required after that date; the Attorney General must also update these capacity requirements as necessary thereafter. Section 104 also prescribes a process under which carriers may identify any systems or services that lack the necessary capacity and obtain reimbursement for any necessary upgrades. *This process has not yet begun for managed VoIP and broadband Internet access providers.* The Commission should not require these providers to modify their networks to implement CALEA capabilities until it is clear what surveillance capacity will be required.

Finally, the Commission correctly observes that entities newly identified as being subject to CALEA will need to develop systems security and integrity policies and procedures under Section 105 that will ensure that interception of communications or call-identifying information may only be conducted pursuant to a court order or other lawful authorization, and with the affirmative intervention of an individual officer of the carrier acting in accordance with regulations prescribed by the FCC. The Commission has established detailed rules implementing Section 105 for telecommunications carriers as defined in the Communications Act of 1934, as amended,[43] but neither these rules nor a timeline for compliance have been developed for the additional entities at issue in this proceeding.

To provide adequate time for entities newly subject to CALEA as a result of any order in this proceeding, the Commission should provide a period of one year from the latest of the dates on which (1) one or more industry associations or standard-setting organizations establish safe

[43] 47 C.F.R. § 64.2100-06.

harbor safeguards that are generally agreed to meet the CALEA capability requirements of Section 103, or the date on which the Commission's order resolving any petitions filed pursuant to Section 107(b) takes effect; (2) the Attorney General issues a final notice of capacity applicable to entities providing any services the Commission finds are subject to CALEA in this proceeding; and (3) the Commission establishes system security and integrity rules applicable to such entities. For satellite-based providers in particular, spectrum scarcity issues make the outcomes of these issues particularly critical in implementing CALEA.

Such a compliance deadline would recognize that, even despite earnest recognition of the law enforcement's surveillance needs, it is simply impossible to build CALEA compliance into a network absent a common understanding on the part of all parties as to what the necessary capabilities are, what capacity will be required, and how system security will be handled. Furthermore, it will minimize the cost to the industry and the Commission alike of preparing and processing myriad petitions for extension of time to comply under Section 107(c) or for determinations that compliance is not reasonable achievable under Section 109(b). In contrast, deadlines that, as the Commission proposes, are unreasonably short (*e.g.*, 90 days), or that do not take into account the parallel processes that must take place, will simply generate a flood of such requests that will needlessly consume untold industry and Commission resources.

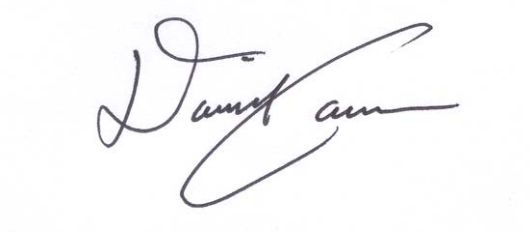
V. CONCLUSION

The *CALEA Broadband NRPM* acknowledges various existing and overlapping CALEA exemptions applicable to some FSS capacity, including bare capacity, services in support of public networks, and interconnection services. The *NPRM* appropriately recognizes limits on the powers delegated by Congress, and thus would expand CALEA coverage only to (1) broadband services; (2) that are provided in the "last mile"; and (3) that replace a substantial portion of the

local telephone exchange service. Unless it meets all three prongs of this test, capacity offered by FSS licensees would not fall within the proposed rule.

The Commission also should consider and, if appropriate, adopt appropriate CALEA satellite broadband guidelines originating from *any* industry association or standards-setting body. Such safe-harbor standards should be platform-independent and based on encoding and transmission protocols used by both satellite-based and terrestrial providers. Finally, the FCC should clarify ambiguous terms and policies as detailed above.

Respectfully submitted,



_____

David Cavossa
Executive Director
Satellite Industry Association

November 8, 2004